

Symbolic Methods for Automated Checking and Generation of Invariant Sets

Khalil Ghorbal

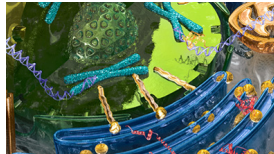
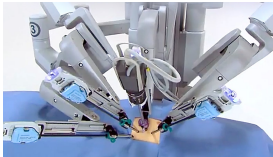
INRIA, France

Joint work with **Andrew Sogokon** and **André Platzer**

NJ, USA

April 24th, 2017

Cyber-Physical Systems



Init

→

[

(

Sensing: read data from sensors

Control: actuate

Plant: evolve ◀◀◀◀◀

)*

]

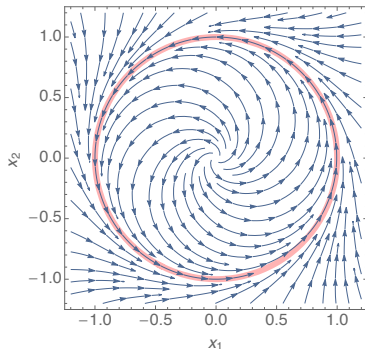
Safety

Evolution

- Continuous time
- Ordinary Differential Equations (ODE)

Qualitative Analysis of Dynamical Systems

$$(\dot{x}_1, \dot{x}_2) = (x_1 - x_1^3 - x_2 - x_1x_2^2, x_1 + x_2 - x_1^2x_2 - x_2^3)$$



**Algebraic
Invariant
Equation**

The solution for $\mathbf{x}_0 = (1, 0)$ respects $\boxed{x_1(t)^2 + x_2(t)^2 - 1 = 0} \quad \forall t$

Numerical Integration & Qualitative Analysis

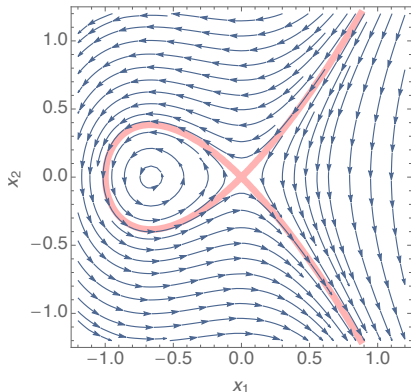
- More precise numerical integration (Geometrical Integration)
- Better understanding of the dynamics without solving the problem (some invariants represent conserved quantities like momentum or energy)

Formal Verification

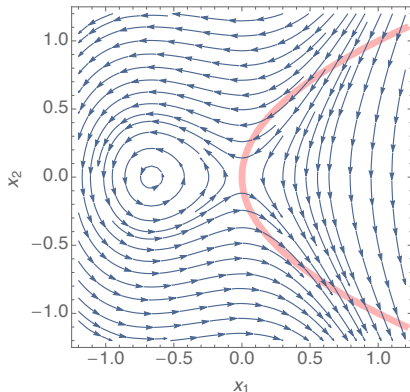
- Formal verification for dynamical and hybrid systems
- Static Analysis (as templates to statically analyze an implementation)
- Safety, Reachability, Stability

Problem I. *Checking Invariance of Algebraic Equations*

Given $\dot{\mathbf{x}} = (-2x_2, -2x_1 - 3x_1^2)$, $p(\mathbf{x}_0) = 0$, is $p(\mathbf{x}(t)) = 0$ for all t ?



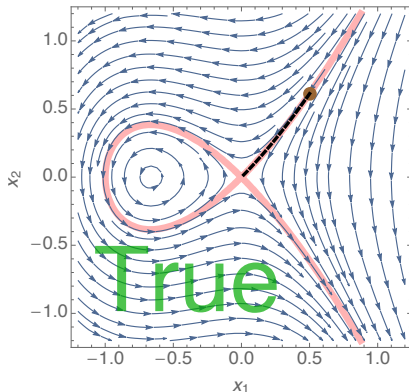
$$p(x_1, x_2) = x_1^2 + x_1^3 - x_2^2$$



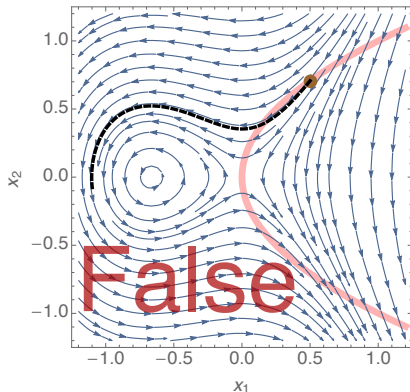
$$p(x_1, x_2) = x_1 - x_2^2$$

Problem I. *Checking Invariance of Algebraic Equations*

Given $\dot{\mathbf{x}} = (-2x_2, -2x_1 - 3x_1^2)$, $p(\mathbf{x}_0) = 0$, is $p(\mathbf{x}(t)) = 0$ for all t ?



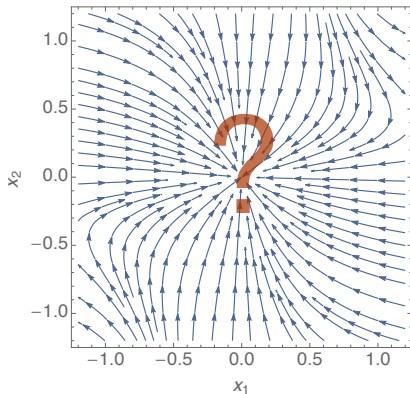
$$p(x_1, x_2) = x_1^2 + x_1^3 - x_2^2$$



$$p(x_1, x_2) = x_1 - x_2^2$$

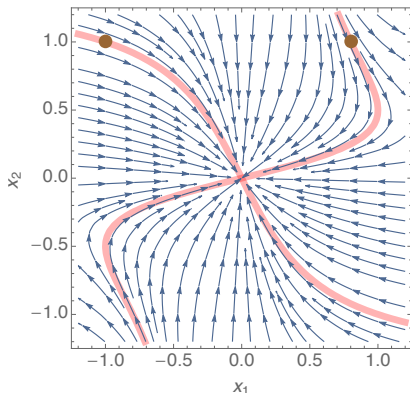
Problem II. *Generate Algebraic Invariant Equations*

Given $\dot{\mathbf{x}} = (-x_1 + 2x_1^2x_2, -x_2)$, how to generate p such that $p(\mathbf{x}(t)) = 0$?



Problem II. *Generate Algebraic Invariant Equations*

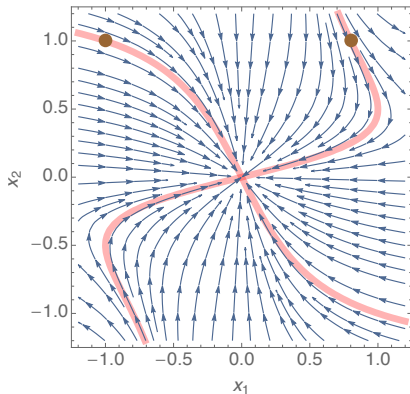
Given $\dot{\mathbf{x}} = (-x_1 + 2x_1^2x_2, -x_2)$, how to generate p such that $p(\mathbf{x}(t)) = 0$?



$$p_{(x_1(0), x_2(0))}(x_1, x_2) = (x_2(0) - x_1(0)x_2(0)^2)x_1 - x_1(0)(x_2 - x_1x_2^2) = 0$$

Problem II. *Generate Algebraic Invariant Equations*

Given $\dot{\mathbf{x}} = (-x_1 + 2x_1^2x_2, -x_2)$, how to generate p such that $p(\mathbf{x}(t)) = 0$?



$$p_{(x_1(0), x_2(0))}(x_1, x_2) = (x_2(0) - x_1(0)x_2(0)^2)x_1 - x_1(0)(x_2 - x_1x_2^2) = 0$$

$\frac{x_1}{x_2 - x_1x_2^2}$ is an invariant **rational function**.

Gradient $\nabla p := \left(\frac{\partial p}{\partial x_1}, \dots, \frac{\partial p}{\partial x_n} \right)$

Lie Derivation $\mathfrak{D}_{\mathbf{f}}(p) := \frac{dp(\mathbf{x}(t))}{dt} = \langle \nabla p, \mathbf{f} \rangle \quad (\dot{\mathbf{x}} = \mathbf{f})$

Singular Locus

$$\text{SL}(p) := \{ \mathbf{x} \in \mathbb{R}^n \mid \nabla p = \mathbf{0} \} = \left\{ \mathbf{x} \in \mathbb{R}^n \mid \frac{\partial p}{\partial x_1} = 0 \wedge \dots \wedge \frac{\partial p}{\partial x_n} = 0 \right\}$$

$\mathbf{x} \in V_{\mathbb{R}}(p)$ ($p(\mathbf{x}) = 0$) is **singular** if $\mathbf{x} \in \text{SL}(p)$, **regular** otherwise.

- 1 Context
- 2 The Checking Problem
- 3 The Generation Problem
- 4 Future Avenues

Notation for “ $S \subseteq \mathbb{R}^n$ is invariant for $\mathbf{f}$ ”

$$S \rightarrow [\dot{\mathbf{x}} = \mathbf{f}]S$$

$\equiv$

The set S is an invariant set for $\mathbf{f}$

$\equiv$

Starting with $\mathbf{x}_0$ s.t $\mathbf{x}_0 \in S$: for all $t > 0$, $\mathbf{x}(t)$
solution of the IVP $(\dot{\mathbf{x}} = \mathbf{f}, \mathbf{x}(0) = \mathbf{x}_0)$ is in S

N.B. Treating $\dot{\mathbf{x}} = \mathbf{f}$ as a program, one can think of the top formula as representing the Hoare triple $\{S\} \dot{\mathbf{x}} = \mathbf{f} \{S\}$.

Notation for “ $S \subseteq \mathbb{R}^n$ is invariant for $\mathbf{f}$ ”

$$S \rightarrow [\dot{\mathbf{x}} = \mathbf{f}]S$$

$\equiv$

The set S is an invariant set for $\mathbf{f}$

$\equiv$

Starting with $\mathbf{x}_0$ s.t $\mathbf{x}_0 \in S$: for all $t > 0$, $\mathbf{x}(t)$
solution of the IVP $(\dot{\mathbf{x}} = \mathbf{f}, \mathbf{x}(0) = \mathbf{x}_0)$ is in S

N.B. Treating $\dot{\mathbf{x}} = \mathbf{f}$ as a program, one can think of the top formula as representing the Hoare triple $\{S\} \dot{\mathbf{x}} = \mathbf{f} \{S\}$.

Notation for “ $S \subseteq \mathbb{R}^n$ is invariant for $\mathbf{f}$ ”

$$S \rightarrow [\dot{\mathbf{x}} = \mathbf{f}]S$$

$\equiv$

The set S is an invariant set for $\mathbf{f}$

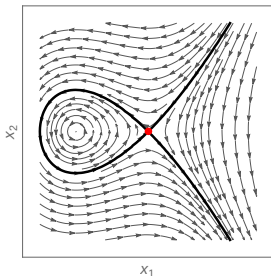
$\equiv$

Starting with $\mathbf{x}_0$ s.t $\mathbf{x}_0 \in S$: for all $t > 0$, $\mathbf{x}(t)$
solution of the IVP $(\dot{\mathbf{x}} = \mathbf{f}, \mathbf{x}(0) = \mathbf{x}_0)$ is in S

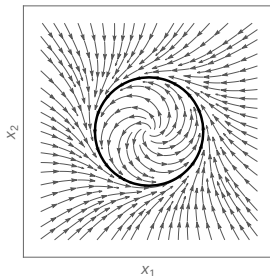
N.B. Treating $\dot{\mathbf{x}} = \mathbf{f}$ as a program, one can think of the top formula as representing the Hoare triple $\{S\} \dot{\mathbf{x}} = \mathbf{f} \{S\}$.

Necessary and sufficient for smooth invariant manifolds (Lie, 1893).

$$\text{(Lie)} \frac{p = 0 \rightarrow (\mathfrak{D}_f(p) = 0 \wedge \nabla p \neq \mathbf{0})}{(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}] (p = 0)}$$



$p = 0$ non-smooth ✗



$p = 0$ smooth ✓

Handling certain **singularities** (points where $\nabla p = \mathbf{0}$)

No flow in the problem variables at singularities on the variety

$$(\text{Lie}^\circ) \frac{p = 0 \rightarrow (\mathcal{D}_{\mathbf{f}}(p) = 0 \wedge (\nabla p = \mathbf{0} \rightarrow \mathbf{f} = \mathbf{0}))}{(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}] \ (p = 0)}$$

Flow at singularities on the variety is directed into the variety

$$(\text{Lie}^*) \frac{p = 0 \rightarrow (\mathcal{D}_{\mathbf{f}}(p) = 0 \wedge (\nabla p = \mathbf{0} \rightarrow p(\mathbf{x} + \lambda \mathbf{f}) = 0))}{(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}] \ (p = 0)} .$$

Handling certain **singularities** (points where $\nabla p = \mathbf{0}$)

No flow in the problem variables at singularities on the variety

$$(\text{Lie}^\circ) \frac{p = 0 \rightarrow (\mathfrak{D}_{\mathbf{f}}(p) = 0 \wedge (\nabla p = \mathbf{0} \rightarrow \mathbf{f} = \mathbf{0}))}{(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}] \ (p = 0)}$$

Flow at singularities on the variety is directed into the variety

$$(\text{Lie}^*) \frac{p = 0 \rightarrow (\mathfrak{D}_{\mathbf{f}}(p) = 0 \wedge (\nabla p = \mathbf{0} \rightarrow p(\mathbf{x} + \lambda \mathbf{f}) = 0))}{(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}] \ (p = 0)} .$$

Handling certain **singularities** (points where $\nabla p = \mathbf{0}$)

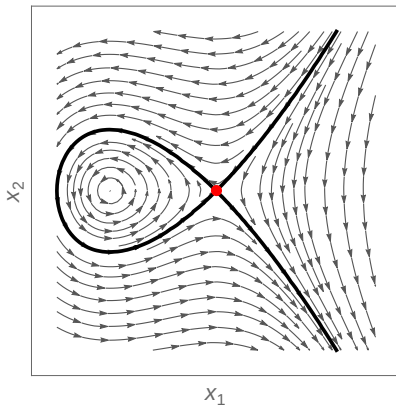
No flow in the problem variables at singularities on the variety

$$(\text{Lie}^\circ) \frac{p = 0 \rightarrow (\mathfrak{D}_{\mathbf{f}}(p) = 0 \wedge (\nabla p = \mathbf{0} \rightarrow \mathbf{f} = \mathbf{0}))}{(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}] (p = 0)}$$

Flow at singularities on the variety is directed into the variety

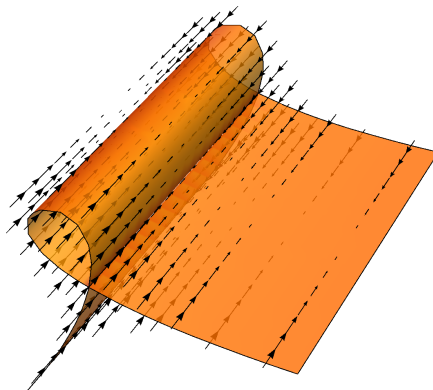
$$(\text{Lie}^*) \frac{p = 0 \rightarrow (\mathfrak{D}_{\mathbf{f}}(p) = 0 \wedge (\nabla p = \mathbf{0} \rightarrow p(\mathbf{x} + \lambda \mathbf{f}) = 0))}{(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}] (p = 0)} .$$

Handling certain **singularities** (points where $\nabla p = \mathbf{0}$)



Lie ✗ Lie° ✓ Lie^* ✓

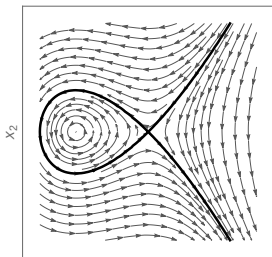
Handling certain **singularities** (points where $\nabla p = \mathbf{0}$)



Lie **X** Lie^o **X** Lie* **✓**

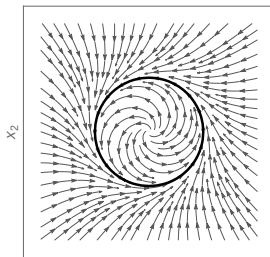
Necessary and sufficient for conserved quantities (integrals of motion).

$$(FI) \frac{\mathfrak{D}_f(p) = 0}{(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}] (p = 0)}$$



x_1

p conserved ✓



x_1

p not conserved ✗

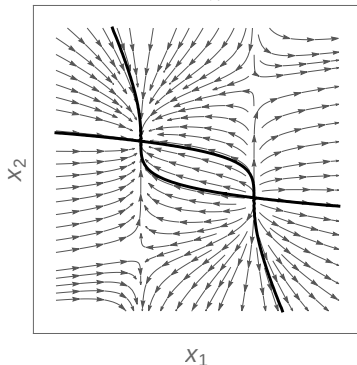
Continuous consecutions (C-c) and **polynomial consecutions** (P-c) are Darboux polynomials (Darboux, 1878).

$$(C-c) \frac{\exists \lambda \in \mathbb{R}, \mathcal{D}_f(p) = \lambda p}{(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}] (p = 0)},$$

$$(P-c) \frac{\exists \lambda \in \mathbb{R}[\mathbf{x}], \mathcal{D}_f(p) = \lambda p}{(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}] (p = 0)}.$$

$$\mathbf{f} = (3(x_1^2 - 4), -x_2^2 + x_1x_2 + 3), \quad p = x_2^4 + 2x_1x_2^3 + 6x_2^2 + 2x_1x_2 + x_1^2 + 3,$$

$$\mathfrak{D}_f(p) = \underbrace{(6x_1 - 4x_2)}_{\lambda} p$$



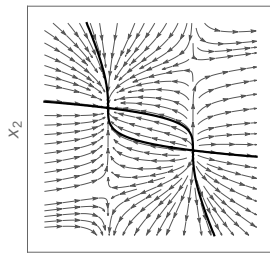
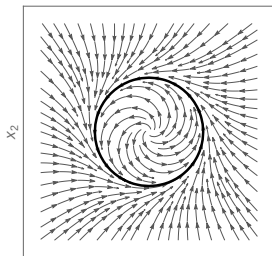
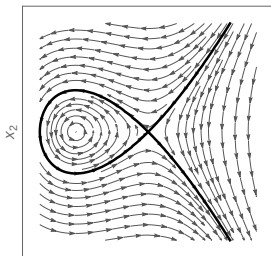
FI ✗ C-c ✗ P-c ✓

Differential Radical Invariants (DRI)

[G. et al., TACAS 2014, SAS 2014]

Necessary and sufficient for invariant varieties.

$$\text{(DRI)} \frac{p = 0 \rightarrow \bigwedge_{i=0}^{N-1} \mathfrak{D}_{\mathbf{f}}^{(i)}(p) = 0}{(p = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}] (p = 0)}$$

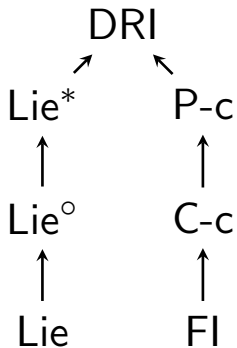


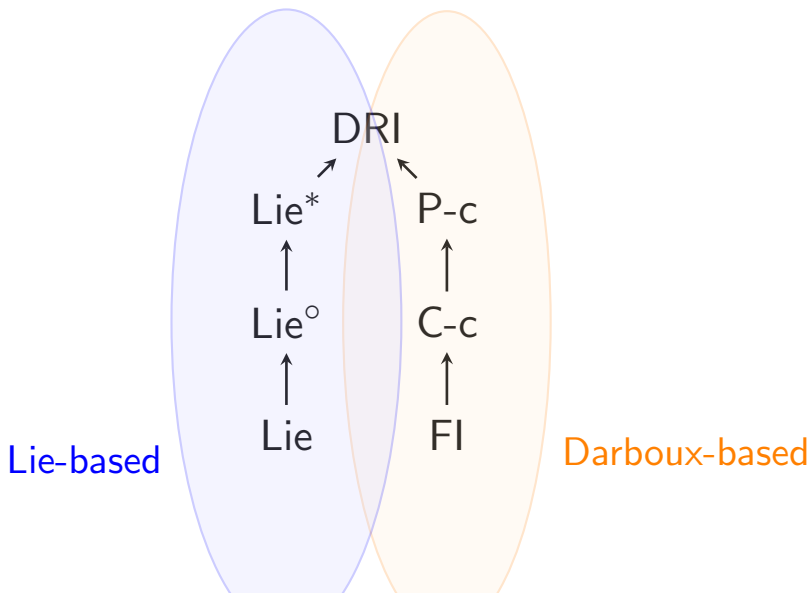
$$(R_A) \frac{A}{S_A : T_A \longrightarrow [\dot{\mathbf{x}} = \mathbf{f}] S_A : T_A} \quad (R_B) \frac{B}{S_B : T_B \longrightarrow [\dot{\mathbf{x}} = \mathbf{f}] S_B : T_B}$$

Partial Order

$R_A \preceq R_B$ if and only if $A \implies B$ and T_A is a “subtype” of T_B .

- $R_A \sim R_B$ ($R_A \preceq R_B$ and $R_A \succeq R_B$) **Equivalence.**
- $R_A \prec R_B$ ($R_A \preceq R_B$ and $R_A \not\succeq R_B$) **Strict increase** of deductive power





Square-free reduction of a polynomial

$$h = h_1^{\alpha_1} h_2^{\alpha_2} \cdots h_k^{\alpha_k}$$

Geometrically $V_{\mathbb{R}}(h) \equiv_{\mathbb{R}} V_{\mathbb{R}}(\text{SF}(h))$.

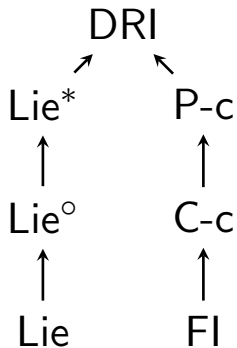
- **SF automated pre-processing** step in **computer algebra** systems
- Is it a “good idea” to apply SF for invariance checking ?

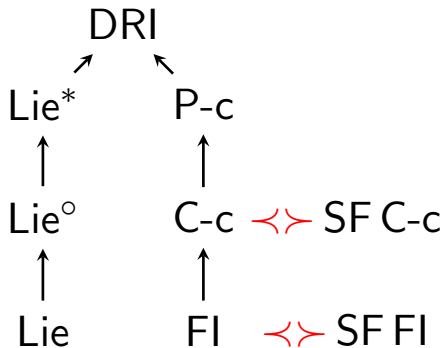
Square-free reduction of a polynomial

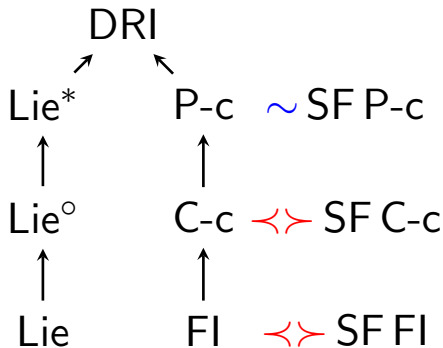
$$\text{SF}(h) = h_1^{\cancel{q_1}} h_2^{\cancel{q_2}} \cdots h_k^{\cancel{q_k}}$$

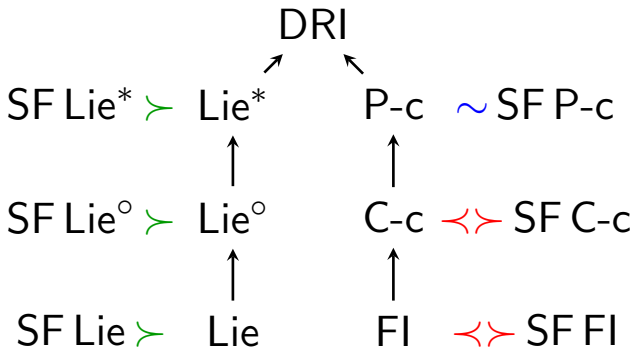
Geometrically $V_{\mathbb{R}}(h) \equiv_{\mathbb{R}} V_{\mathbb{R}}(\text{SF}(h))$.

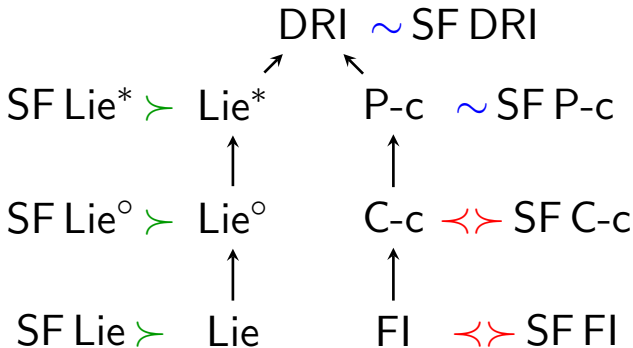
- SF **automated pre-processing** step in **computer algebra** systems
- Is it a “good idea” to apply SF for invariance checking ?











So far we have only seen **algebraic** sets: $p = 0$

- For $\wedge_i p_i = 0$, we can rewrite using $\sum_i p_i^2 = 0$
- We can do better [SAS'14]

What about **semi-algebraic** sets:

- Sets of the form $p \leq 0$
- Closed Sets
- Arbitrary Sets: boolean formulae with polynomial equalities and inequalities

Sub-tangent Vector

A vector $\mathbf{v} \in \mathbb{R}^n$ is sub-tangential to a set $S \subseteq \mathbb{R}^n$ at $\mathbf{x} \in S$ if

$$\liminf_{\lambda \rightarrow 0^+} \frac{\text{dist}(S, \mathbf{x} + \lambda \mathbf{v})}{\lambda} = 0. \quad (\text{dist}(S, \mathbf{x}) \equiv \inf_{\mathbf{y} \in S} \|\mathbf{x} - \mathbf{y}\|_1)$$

Contingent Cone

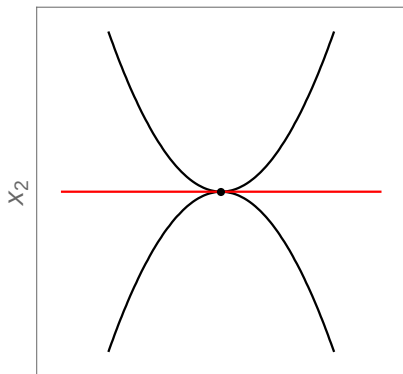
$K_{\mathbf{x}}(S)$: the set of all sub-tangent vectors to a set S at $\mathbf{x} \in S$.

Nagumo's Theorem

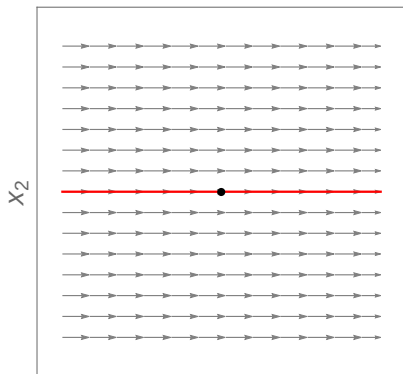
A **closed** set $S \subset \mathbb{R}^n$ is **positively invariant** under the flow of the system if and only if $\mathbf{f}(\mathbf{x}) \in K_{\mathbf{x}}(S)$ for all $\mathbf{x} \in \text{bdr}(S)$ (boundary of S).

Contingent Cone of Boolean Formulae

$$K_x(S_1) \cap K_x(S_2) \supset K_x(S_1 \cap S_2)$$



$$x_2 + x_1^2 = 0 \wedge x_2 - x_1^2 = 0$$



$$\dot{x}_1 = 1, \dot{x}_2 = 0$$

(Non-strict) Barrier Certificate ✓

$(\forall \mathbf{x} \in \mathbb{R}^n, \mathfrak{D}_{\mathbf{f}}(p) \leq 0) \longrightarrow p \leq 0$ is a positive invariant

Unsound Barrier Certificate ✗

$(\forall \mathbf{x} \text{ s.t. } \mathbf{p}(\mathbf{x}) = \mathbf{0}, \mathfrak{D}_{\mathbf{f}}(p) \leq 0) \longrightarrow p \leq 0$ is a positive invariant

Strict Barrier Certificate ✓

$(\forall \mathbf{x} \text{ s.t. } p(\mathbf{x}) = 0, \mathfrak{D}_{\mathbf{f}}(\mathbf{p}) < \mathbf{0}) \longrightarrow p \leq 0$ is a positive invariant

Differential Invariants (DI)

$$(DI) \frac{D(S)_{\dot{\mathbf{x}}}^{\mathbf{f}}}{S \rightarrow [\dot{\mathbf{x}} = \mathbf{f}] S},$$

$D(S)_{\dot{\mathbf{x}}}^{\mathbf{f}}$: substitute each $\dot{x}_i$ in $D(S)$ with $\mathbf{f}_i(\mathbf{x})$

$$D(r) = 0 \quad \text{for numbers,}$$

$$D(x) = \dot{x} \quad \text{for variables,}$$

$$D(a + b) = D(a) + D(b),$$

$$D(a \cdot b) = D(a) \cdot b + a \cdot D(b),$$

$$D(a \leq b) \equiv D(a) \leq D(b), \quad \text{accordingly for } \geq, >, < . \text{ (BC)}$$

$$D(S_1 \wedge S_2) \equiv D(S_1) \wedge D(S_2),$$

$$D(S_1 \vee S_2) \equiv D(S_1) \wedge D(S_2), \quad (\wedge \text{ here is important for soundness})$$

Non-smooth Strict Barrier Certificate (NSSBC)

Apply Strict Barrier Certificate on Active Boundaries

$$\text{(NSSBC)} \quad \frac{\left(\min_{i=1,\dots,k} \max_{j=1,\dots,m(i)} p_{ij} = 0 \right) \rightarrow \mathfrak{D}_{\mathbf{f}} \left(\min_{i=1,\dots,k} \max_{j=1,\dots,m(i)} p_{ij} \right) < 0}{\left(\bigvee_{i=1}^k \bigwedge_{j=1}^{m(i)} p_{ij} \leq 0 \right) \rightarrow [\dot{\mathbf{x}} = \mathbf{f}] \left(\bigvee_{i=1}^k \bigwedge_{j=1}^{m(i)} p_{ij} \leq 0 \right)}.$$

Check Invariance of $p_1 \leq 0 \vee p_2 \leq 0$

NSSBC

$$\begin{aligned} & (p_1 < p_2 \wedge p_1 = 0 \rightarrow \mathfrak{D}_{\mathbf{f}}(p_1) < 0) \\ \wedge & (p_1 > p_2 \wedge p_2 = 0 \rightarrow \mathfrak{D}_{\mathbf{f}}(p_2) < 0) \\ \wedge & (p_1 = p_2 = 0 \rightarrow \mathfrak{D}_{\mathbf{f}}(p_1) < 0 \vee \mathfrak{D}_{\mathbf{f}}(p_2) < 0) \end{aligned}$$

DI

$$\mathfrak{D}_{\mathbf{f}}(p_1) \leq 0 \wedge \mathfrak{D}_{\mathbf{f}}(p_2) \leq 0$$

Definitions

$$\text{In}_f(S) \equiv \{\mathbf{x} \in \mathbb{R}^n \mid \exists \epsilon > 0. \forall t \in (0, \epsilon). \mathbf{x}(t) \in S\},$$

$$\text{In}_{(-f)}(S) \equiv \{\mathbf{x} \in \mathbb{R}^n \mid \exists \epsilon > 0. \forall t \in (0, \epsilon). \mathbf{x}(-t) \in S\},$$

Characterization

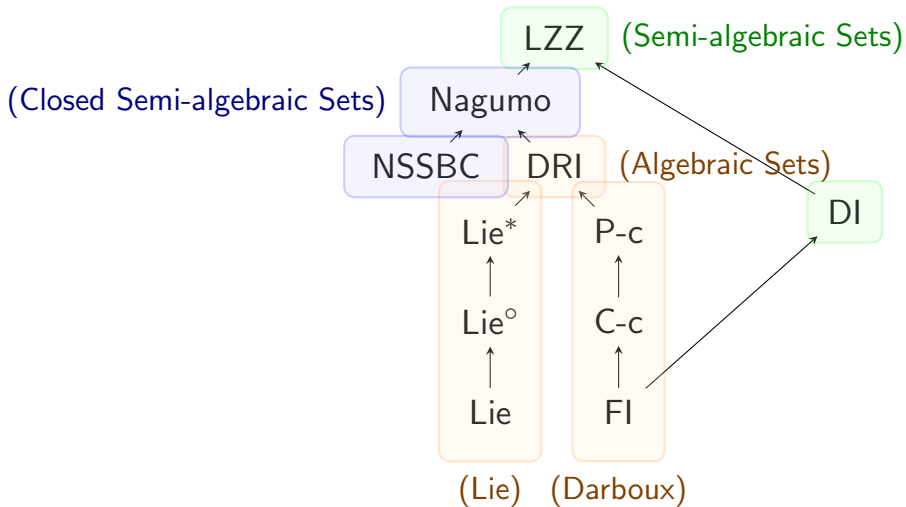
An arbitrary set $S \subset \mathbb{R}^n$ is a positive invariant for $\mathbf{f}$ if and only if

$$S \subseteq \text{In}_f(S) \text{ and } S^c \subseteq \text{In}_{(-f)}(S^c)$$

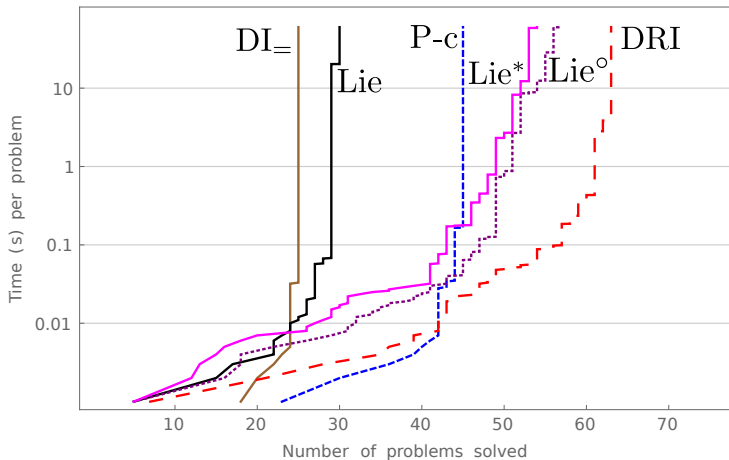
or equivalently

$$\text{In}_{(-f)}(S) \subseteq S \subseteq \text{In}_f(S)$$

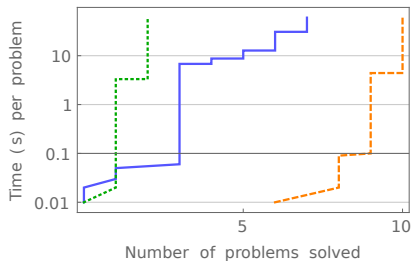
- $\text{In}_f(S)$ can be computed using high-order Lie derivatives !



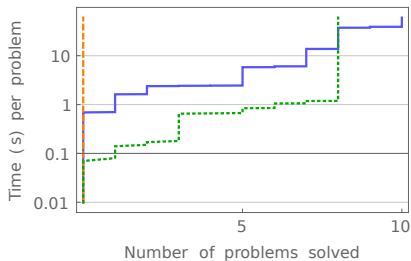
Experimental Performance: Algebraic Sets



Experimental Performance: Semi-algebraic Sets



LZZ vs DI



LZZ vs NSSBC

— LZZ - - - DI . . . NSSBC

- 1 Context
- 2 The Checking Problem
- 3 The Generation Problem**
- 4 Future Avenues

Template-Based

- Fix a template: generic polynomials with symbolic coefficients
- Use sufficient conditions to derive constraints over the coefficients
- Solve the system
- In practice:
 - templates of the form $p = 0$ (algebraic sets) with Darboux condition ($\mathcal{D}_f(p) \in \langle p \rangle$) work for $n \leq 10$ and $d \leq 3$.
 - templates of the form $p \leq 0$ relying on Barrier Certificates (SOSTools)

Discrete Abstraction

- Discrete the space with the signs of a given set of polynomials
- Relies on sufficient conditions to remove spurious transitions
- Issue: How to populate and eventually refine the initial set of polynomials

Suppose we have a 2-dimensional ODE $(\dot{x}_1, \dot{x}_2) = (x_1, x_2)$

Suppose we have a 2-dimensional ODE $(\dot{x}_1, \dot{x}_2) = (x_1, x_2)$

- 1 Start with parametric h of degree 1: $h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$

Suppose we have a 2-dimensional ODE $(\dot{x}_1, \dot{x}_2) = (x_1, x_2)$

- 1 Start with parametric h of degree 1: $h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$
- 2 Start with $N = 1$

Suppose we have a 2-dimensional ODE $(\dot{x}_1, \dot{x}_2) = (x_1, x_2)$

- 1 Start with parametric h of degree 1: $h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$
- 2 Start with $N = 1$
- 3 Find $\beta \in \mathbb{R}$ such that: $\mathfrak{D}_f(h) = \beta h$

Suppose we have a 2-dimensional ODE $(\dot{x}_1, \dot{x}_2) = (x_1, x_2)$

- 1 Start with parametric h of degree 1: $h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$
- 2 Start with $N = 1$
- 3 Find $\beta \in \mathbb{R}$ such that: $\mathfrak{D}_f(h) = \beta h$

$$\mathfrak{D}_f(h) = \alpha_1 x_1 + \alpha_2 x_2 = \beta(\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3)$$

Suppose we have a 2-dimensional ODE $(\dot{x}_1, \dot{x}_2) = (x_1, x_2)$

- 1 Start with parametric h of degree 1: $h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$
- 2 Start with $N = 1$
- 3 Find $\beta \in \mathbb{R}$ such that: $\mathfrak{D}_f(h) = \beta h$

$$\mathfrak{D}_f(h) = \alpha_1 x_1 + \alpha_2 x_2 = \beta(\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3)$$

$$\begin{array}{rcl} (-1 + \beta)\alpha_1 & = & 0 \\ (-1 + \beta)\alpha_2 & = & 0 \\ (\beta)\alpha_3 & = & 0 \end{array} \Leftrightarrow \begin{pmatrix} -1 + \beta & 0 & 0 \\ 0 & -1 + \beta & 0 \\ 0 & 0 & \beta \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = 0$$

Suppose we have a 2-dimensional ODE $(\dot{x}_1, \dot{x}_2) = (x_1, x_2)$

- 1 Start with parametric h of degree 1: $h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$
- 2 Start with $N = 1$
- 3 Find $\beta \in \mathbb{R}$ such that: $\mathfrak{D}_f(h) = \beta h$

$$\mathfrak{D}_f(h) = \alpha_1 x_1 + \alpha_2 x_2 = \beta(\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3)$$

$$\begin{aligned} (-1 + \beta)\alpha_1 &= 0 \\ (-1 + \beta)\alpha_2 &= 0 \\ (\beta)\alpha_3 &= 0 \end{aligned} \Leftrightarrow \begin{pmatrix} -1 + \beta & 0 & 0 \\ 0 & -1 + \beta & 0 \\ 0 & 0 & \beta \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = 0$$

Study the **null space** (kernel) of $M(\beta)$

$$h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$$

$$\begin{aligned} (-1 + \beta)\alpha_1 &= 0 \\ (-1 + \beta)\alpha_2 &= 0 \\ (\beta)\alpha_3 &= 0 \end{aligned} \Leftrightarrow \begin{pmatrix} -1 + \beta & 0 & 0 \\ 0 & -1 + \beta & 0 \\ 0 & 0 & \beta \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = 0$$

Study the **null space** (kernel) of $M(\beta)$

- Max dim of ker of $M(\beta) \rightsquigarrow$ more freedom for $\alpha = (\alpha_1, \alpha_2, \alpha_3)$
- Increases the chances of finding **first integrals**
- Dually, minimize the rank of $M(\beta)$

$$h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$$

$$\begin{aligned} (-1 + \beta)\alpha_1 &= 0 \\ (-1 + \beta)\alpha_2 &= 0 \\ (\beta)\alpha_3 &= 0 \end{aligned} \Leftrightarrow \begin{pmatrix} -1 + \beta & 0 & 0 \\ 0 & -1 + \beta & 0 \\ 0 & 0 & \beta \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = 0$$

Study the **null space** (kernel) of $M(\beta)$

- Max dim of ker of $M(\beta) \rightsquigarrow$ more freedom for $\alpha = (\alpha_1, \alpha_2, \alpha_3)$
- Increases the chances of finding **first integrals**
- Dually, minimize the rank of $M(\beta)$

$$h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$$

$$\begin{aligned} (-1 + \beta)\alpha_1 &= 0 \\ (-1 + \beta)\alpha_2 &= 0 \\ (\beta)\alpha_3 &= 0 \end{aligned} \Leftrightarrow \begin{pmatrix} -1 + \beta & 0 & 0 \\ 0 & -1 + \beta & 0 \\ 0 & 0 & \beta \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = 0$$

Study the **null space** (kernel) of $M(\beta)$

- Max dim of $\ker$ of $M(\beta) \rightsquigarrow$ more freedom for $\alpha = (\alpha_1, \alpha_2, \alpha_3)$
- Increases the chances of finding **first integrals**
- Dually, minimize the rank of $M(\beta)$

$$h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$$

$$\begin{aligned} (-1 + \beta)\alpha_1 &= 0 \\ (-1 + \beta)\alpha_2 &= 0 \\ (\beta)\alpha_3 &= 0 \end{aligned} \Leftrightarrow \begin{pmatrix} -1 + \beta & 0 & 0 \\ 0 & -1 + \beta & 0 \\ 0 & 0 & \beta \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = 0$$

Study the **null space** (kernel) of $M(\beta)$

- Max dim of ker of $M(\beta)$ $\rightsquigarrow$ more freedom for $\alpha = (\alpha_1, \alpha_2, \alpha_3)$
- Increases the chances of finding **first integrals**
- Dually, minimize the rank of $M(\beta)$ $\rightsquigarrow$ **NP-hard** [Buss et al. 1999]

$$h = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3$$

$$\begin{aligned} (-1 + \beta)\alpha_1 &= 0 \\ (-1 + \beta)\alpha_2 &= 0 \\ (\beta)\alpha_3 &= 0 \end{aligned} \Leftrightarrow \begin{pmatrix} -1 + \beta & 0 & 0 \\ 0 & -1 + \beta & 0 \\ 0 & 0 & \beta \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = 0$$

Study the **null space** (kernel) of $M(\beta)$

- Max dim of ker of $M(\beta) \rightsquigarrow$ more freedom for $\alpha = (\alpha_1, \alpha_2, \alpha_3)$
- Increases the chances of finding **first integrals**
- Dually, minimize the rank of $M(\beta) \rightsquigarrow$ **NP-hard** [Buss et al. 1999]

$$h = x_2(0)x_1 - x_1(0)x_2$$

- 1 Context
- 2 The Checking Problem
- 3 The Generation Problem
- 4 Future Avenues**

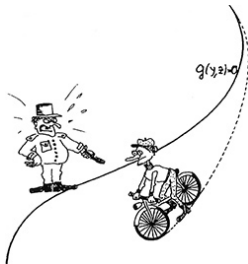
Challenges



- Verification and Faithful Simulation for cyber-physical systems with DAE

Differential-Algebraic Equations (DAE)

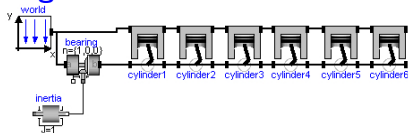
- Verification and Faithful Simulation for cyber-physical systems with DAE



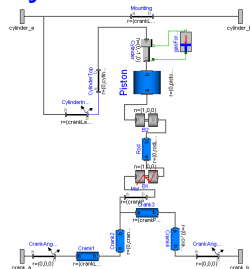
- $0 = F(x, \dot{x}, t)$
- $\begin{cases} \dot{x} = f(y, x) \\ 0 = g(y, x) \end{cases}$
- Compositional design
- Tools: Dymola (Dassault Systèmes), Modelica

V6 Engine Simple Combustion Model (Modelica)

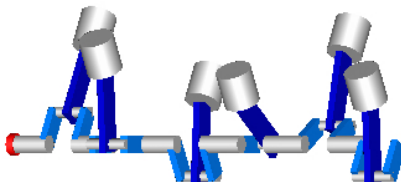
Engine



Cylinder



Simulation



Invariants Generation for DAE

- Extends previous work (algebraic approach)
- Semi-explicit form of index 1 (specific class of DAE)

Hybrid Simulation is Hard

- Well-founded operational semantics (compilation, index reduction)
 - Preserve compositionality in presence of mode changes
 - Proper handling of zero-crossing (detection and consistent initialization)
 - Cascades of zero-crossings (sliding modes)
- ➡ Investigate the use of **static analysis** and **symbolic computation**

Invariants Generation for DAE

- Extends previous work (algebraic approach)
- Semi-explicit form of index 1 (specific class of DAE)

Hybrid Simulation is Hard

- Well-founded operational semantics (compilation, index reduction)
- Preserve compositionality in presence of mode changes
- Proper handling of zero-crossing (detection and consistent initialization)
- Cascades of zero-crossings (sliding modes)

➡ Investigate the use of **static analysis** and **symbolic computation**

Invariants Generation for DAE

- Extends previous work (algebraic approach)
- Semi-explicit form of index 1 (specific class of DAE)

Hybrid Simulation is Hard

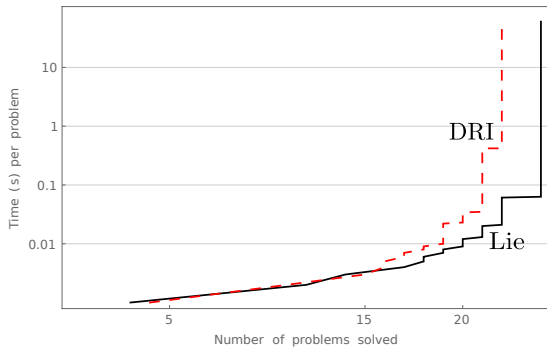
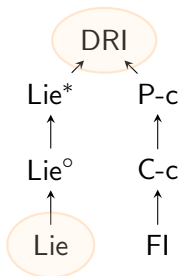
- Well-founded operational semantics (compilation, index reduction)
 - Preserve compositionality in presence of mode changes
 - Proper handling of zero-crossing (detection and consistent initialization)
 - Cascades of zero-crossings (sliding modes)
- ➔ Investigate the use of **static analysis** and **symbolic computation**

Thanks for your attention !



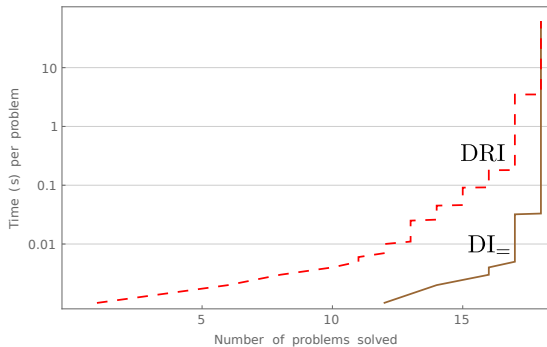
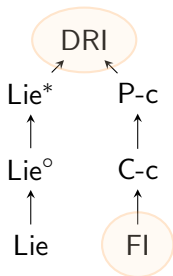
Smooth invariant manifolds (Lie vs DRI)

Lie and DRI **decide** invariance for **smooth invariant manifolds**.



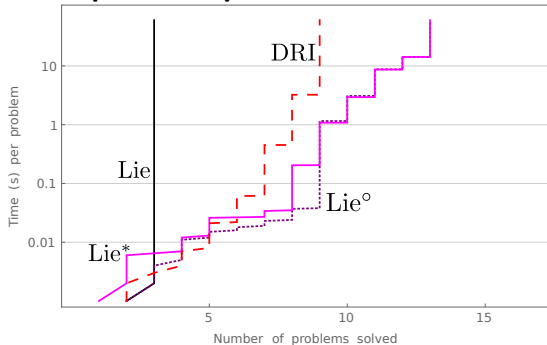
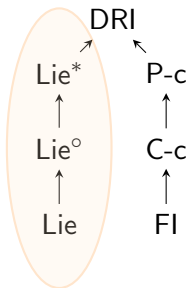
Functional invariants (DI vs DRI)

DI₌ and DRI **decide** invariance of varieties of **conserved quantities**.



Singularities at Equilibria (Lie , Lie° & Lie^* vs DRI)

Lie° , Lie^* and DRI **decide** invariance for varieties of with **singularities that are equilibrium points**.



$$\begin{aligned}
& (h_1 > \max(h_2, \dots, h_m) \rightarrow \mathcal{D}_f(h_1) < 0) \\
\wedge \quad & (h_1 < \max(h_2, \dots, h_m) \rightarrow \mathcal{D}_f(\max(h_2, \dots, h_m)) < 0) \\
\wedge \quad & (h_1 = \max(h_2, \dots, h_m) \rightarrow \mathcal{D}_f(h_1) < 0 \wedge \mathcal{D}_f(\max(h_2, \dots, h_m)) < 0)
\end{aligned}$$

$$\begin{aligned}
& (g_1 < \min(g_2, \dots, g_m) \rightarrow \mathcal{D}_f(g_1) < 0) \\
\wedge \quad & (g_1 > \min(g_2, \dots, g_m) \rightarrow \mathcal{D}_f(\min(g_2, \dots, g_m)) < 0) \\
\wedge \quad & (g_1 = \min(g_2, \dots, g_m) \rightarrow \mathcal{D}_f(g_1) < 0 \vee \mathcal{D}_f(\min(g_2, \dots, g_m)) < 0)
\end{aligned}$$